



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 779 760 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.06.1997 Bulletin 1997/25

(51) Int Cl. 6: H04Q 7/32

(21) Application number: 96660094.2

(22) Date of filing: 09.12.1996

(84) Designated Contracting States:
DE FR GB SE

• Paajanen, Reijo
33820 Tampere (FI)

(30) Priority: 15.12.1995 FI 956036

• Rautiola, Markku
33720 Tampere (FI)

(71) Applicant: NOKIA MOBILE PHONES LTD.
24101 Salo (FI)

• Rossi, Markku
41160 Tikkakoski (FI)

(72) Inventors:

- Hämäläinen, Jari
33720 Tampere (FI)

(74) Representative: Pursialinen, Timo Pekka et al
Tampereen Patenttitöimisto Oy,
Hermiankatu 6
33720 Tampere (FI)

(54) Method for indicating enciphering of data transmission between a mobile communication network and a mobile station

(57) The invention relates to a method for indicating enciphering of data transmission between a mobile communication network and a mobile station (MS) in the mobile communication network, wherein signals trans-

ferred between a mobile communication network and a mobile station are monitored, and on the basis of the signal monitored, the cipher mode is indicated to the user of the mobile station.

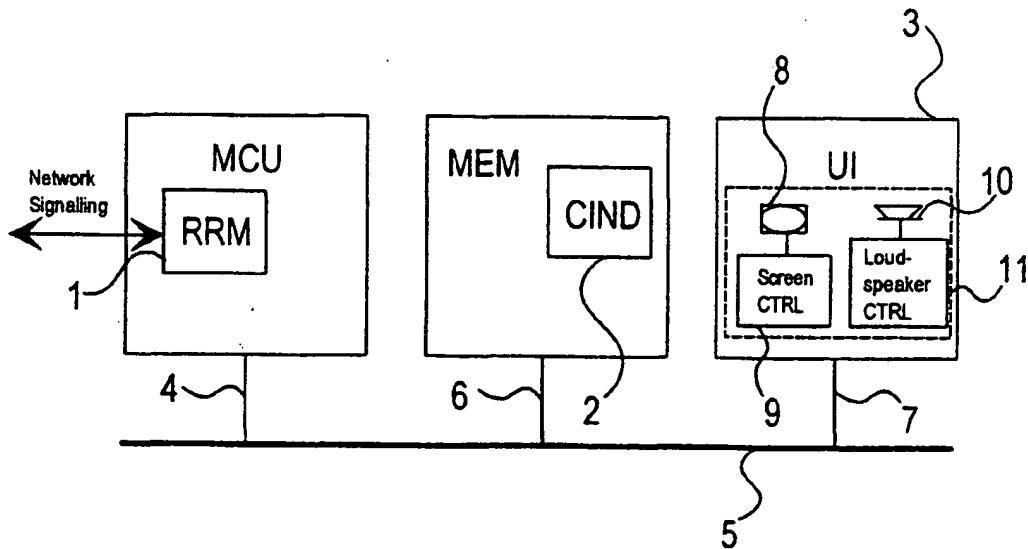


Fig. 5

Description

The invention relates to a method and an apparatus for indicating enciphering of data transmission between a mobile communication network and a mobile station in the mobile communication network.

In mobile networks, at least part of the data transmission is wireless communication using radio transmitters and receivers. The radio channel is a physically open resource available to anyone by means of suitable communication equipment. This involves security risks, such as eavesdropping or disclosure of privacy of location. In digital mobile networks, such as GSM networks, digital data transmission is used which is difficult to eavesdrop. Further, it is possible to use identification of the caller and enciphering in data transmission. For preventing eavesdropping in digital mobile networks, enciphering methods have been developed for enciphering the speech and data signals modified in digital form. Moreover, enciphering can be used in the transmission of other information via the radio channel, such as identification data on the mobile station (International Mobile Subscriber Identity, IMSI) and on the location (Location Area Identification, LAI). In the receiver, the enciphered signal is decoded back to deciphered speech and data. A so-called encryption key and algorithm are advantageously known to the respective sending and receiving devices only, wherein given the effective encryption algorithms presently in use, decoding a coded signal to intelligible speech and data as well as into processing signals of the bit stream by force or illegally, i.e. without the correct encryption key and algorithm, is practically impossible.

The most common digital mobile networks are cellular networks. The base station subsystem (BSS) of the mobile network comprises base transceiver stations (BTS) and base station controllers (BSC). The mobile station (MS) communicates via the radio channel with a base station close to the respective location of the mobile station. The base station communicates with the base station controller. Data transmission between the base station and the base station controller takes place usually via a cable. One base station controller controls over a group of several base stations. The base station controller, in turn, communicates with a mobile services switching centre (MSC). Several mobile services switching centres, in turn, can communicate with each other as well as with a landline communication network centre (PSTN, ISDN). The information to be transmitted is usually divided into frames containing control information, speech and data converted into digital form, and error correction information. The frame structure can have several levels, wherein frames of a higher level are formed by arranging frames of a lower level. Enciphering can be used both with control information and with speech and data. Moreover, enciphering can be realized by using different encryption keys and algorithms at different frame levels. An example of a digital data trans-

mission network is the GSM network, the standard of which contains definitions of the enciphering methods and algorithms to be used.

In the GSM network, making a mobile-originated call is conducted in a way that a GSM mobile station and the GSM system network give signals, i.e. transmit control and identification information required for making a call. In response to a request for a connection, the GSM mobile station is allotted a channel for signalling, if this is possible within the capacity of the GSM system network. On this channel, the GSM mobile station requests speech or data service from the GSM system network. On the side of the GSM system network, this request is transmitted to a mobile services switching centre (MSC), where the rights of the GSM subscriber are checked from a visitor location register (VLR).

Upon a mobile-terminated call e.g. from a subscription of a landline telephone network, the operator of the telephone network transmits e.g. the number of the receiving telephone to the mobile services switching centre. The mobile services switching centre finds out the rights of the GSM subscriber from the home location register (HLR) and from the visitor location register (VLR). After this, the GSM system network and the GSM mobile station transmit the control and identification information required for making a call.

Depending on the implementation and the configuration of the parameters, the visitor location register VLR can make a request via the mobile services switching centre to the GSM mobile station for exchange of identification information and start of enciphering. This request is made in a so-called cipher mode command message. It is, however, possible to make a call also without exchange of identification information and enciphering. In other words, the call is either enciphered or not enciphered depending on the network parameters set by the GSM system network operator.

In most common mobile communication networks currently available, however, enciphering is not optional to a user of the mobile communication network but usually an alternative function offered by the operator of the mobile network, wherein when current wireless data transmission equipment is used, the user has no certainty whether the data transmission is enciphered or not. Particularly when the mobile station is moving, the mobile station can be transferred from the area of one base station system to the area of another base station system, wherein the cipher mode of data transmission can be changed.

One purpose of the present invention is to eliminate the disadvantages described above and to provide a method for indicating enciphering of data transmission to the user of the mobile communication network. The invention is based on the idea that control signals used in data transmission between a mobile network and a mobile station are monitored and when a control signal for enciphering is detected, the cipher mode is signalled with a cipher mode indicator connected to the mobile

station. The method of the invention is characterized in that signals transferred between a mobile communication network and a mobile station are monitored, and on the basis of the signal monitored, the cipher mode is indicated to the user of the mobile station.

The apparatus according to the invention is characterized in that the apparatus comprises means for monitoring signals transferred between a mobile communication network and a mobile station, and means for indicating the cipher mode to the user of the mobile station.

The invention gives significant advantages. Using the method of the invention, the user of a data transmission device is always aware of whether the data transmission is enciphered or not. Further, by using the method of the invention, it is possible to indicate a possible change in the cipher mode during the data transmission to the user of the data transmission device.

In the following, the invention will be described in more detail with reference to the appended drawings. In the drawings,

Fig. 1a shows the call set-up signals during a mobile-originated call in the GSM mobile communication network,

Fig. 1b shows the call set-up signals during a mobile-terminated call in the GSM mobile communication network,

Fig. 2 is a reduced signal chart on detection of the cipher mode by the principle of interrupting,

Fig. 3 is a reduced signal chart on an enquiry about the cipher mode,

Fig. 4 is a reduced signal chart on detection of the cipher mode when enquiries at regular intervals are used,

Fig. 5 is a reduced block diagram showing the location of the most essential blocks of a cipher mode indicating device in a mobile station according to an advantageous embodiment of the invention,

Fig. 6 is a reduced block diagram showing the implementation of a cipher mode indicating device in connection with a mobile station and a data processor,

Fig. 7 is a reduced chart on a situation where a data transmission connection is formed between two mobile stations, and

Fig. 8 is a reduced signal chart on an enquiry about the cipher mode in a situation where a data transmission connection is formed between

two mobile stations.

Figure 1a shows call set-up signalling during a mobile-originated call and Fig. 1b shows call set-up signals during a mobile-terminated call in the GSM mobile communication network. During call set-up signalling, enciphering information is exchanged if the cipher mode is set on. Upon call set-up signalling, the mobile communication network sends a cipher mode command message requesting the mobile station MS to start enciphering. When the mobile station MS receives this message, it sets a cipher indication data field CIND to show that the cipher mode is on. The cipher indication data field CIND used can be e.g. a predetermined binary digit. Thus the value of the binary digit can be either a logical "0" or a logical "1". For example in logical circuits having an operating voltage of 3 V, the logical "0" value corresponds advantageously to a voltage value of approximately 0V and the logical "1" value corresponds to a voltage of approximately 3 V, which is known as such. The cipher indication data field CIND used can be naturally any other data field as well, such as a byte, wherein advantageously when the value of the byte is zero, the cipher mode is off and, in a corresponding manner, when the value of the byte is different from zero, the cipher mode is on. The contents of the cipher indication data field CIND is cleared upon starting up the mobile station MS and always after a call has been ended. When the user starts a new call and the call set-up signalling advances, the value of the cipher indication data field CIND is changed in connection with the exchange of ciphering information to be different from zero, i.e. to indicate that the cipher mode is on.

Now referring to Fig. 2, when the resource control block 1 of the mobile station MS detects a cipher control signal in the communication between the mobile station and the base station, the resource control block sets the value of the cipher indication data field CIND in a cipher indicator memory block 2 to correspond with the cipher indication data. The cipher indicator memory block 2 reads the value of the cipher indication data field and detects that a new value has been set in it, wherein the cipher indicator memory block 2 makes a request for interruption. A user interface block 3 detects the request for interruption, wherein it sends an enquiry on the cipher mode to the cipher indicator memory block 2 which returns the data on the cipher mode to the user interface block 3. Following this, the user interface block 3 sets the cipher indicator to the mode corresponding to the ciphering data, for example with a certain sign on the display of the mobile station. The change of the cipher mode can also be indicated with an acoustic signal, wherein the user notices the change in the cipher mode also when talking to a mobile station. Thus the user does not need to have visual contact with the display of the mobile station. The user of the mobile station is informed of the cipher mode at the beginning of and during the call. This is important particularly in situations where the

cipher mode can be changed during the call, for example when the mobile station is moving.

Figure 3 illustrates a second advantageous embodiment of the method according to the invention. Here the difference to the embodiment of Fig. 2 lies primarily in that a change in the cipher indication data field does not lead to a request for interruption but the cipher indicator memory block 2 sends the cipher information to the user interface block 3 whenever the value in the cipher indicator memory block is changed. In other respects, the operation of the embodiment shown in Fig. 3 corresponds substantially to the operation of the embodiment shown in Fig. 2.

Figure 4 illustrates a third advantageous embodiment of the method according to the invention, wherein the user interface block 3 sends cipher mode enquiry messages at regular intervals to the cipher indicator memory block 2. The cipher indicator memory block 2 sends a response to the enquiry to the user interface block 3 which will transmit the cipher information to the cipher indicator. In this embodiment, a separate message on the change in the cipher indication data field is not formed. When using this embodiment, the interval of sending enquiry messages must be kept sufficiently short in order to detect a change in the cipher mode sufficiently quickly. In this embodiment, it is advantageous to form a cipher mode enquiry message at least in those situations when the mobile station moves from the area of one base station system to the area of another base station system.

During a call, it is possible to transmit so-called short message services (SMS) to the mobile station. In the transmission of short messages, the cipher mode may deviate from the cipher mode of the call in question, wherein the method of the invention can be used to indicate the cipher mode separately for the call and for the short message services. Also a change in the cipher mode can be indicated to the user both for the call and for the short message services. For indicating the cipher mode and a change in the cipher mode, signals distinguishable from each other can be used, e.g. different acoustic signals, wherein the user of the mobile station is aware of the cipher mode of both the call and the short message services.

The method according to the present invention can also be applied in a way that the existence of enciphering is indicated to the user already before starting the call. This can be implemented advantageously by providing the menu structure of the mobile station with a function whereby the user can ask the mobile communication network about the cipher mode. When this function is selected from the menu, the mobile station sends the mobile network a message inquiring the cipher mode. In practice, this can be conducted in the GSM mobile network by forcing the mobile station to a location update procedure. This procedure contains starting of enciphering if the cipher mode is active in the mobile communication network. In this way, the mobile station

can send to the mobile communication network an enquiry about the current cipher mode, which is indicated to the user e.g. by an icon in the display of the mobile station.

5 Problems may result in countries where enciphering is not allowed to be on during speech because of legislation or for another reason. However, enciphering can thus be on for signalling, i.e. the location update procedure shows cipher-on mode although it is not on for speech. Thus the mobile station can produce an acoustic signal when it turns on the speech channel and detects a change in the cipher mode, wherein the user will be informed that speech is not transferred in enciphered form.

10 15 Figure 5 is a reduced block diagram showing one embodiment of the apparatus according to the invention. A functional part of the central processing unit MCU consists of the resource control block 1 which processes signalling between the mobile communication network and the mobile station. The resource control block 1 is in a transmission connection via a first signal bus 4 to a data transmission bus 5. The data transmission bus 5 is connected with a memory block MEM by means of a second signal bus 6. Further, the data transmission bus 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230 235 240 245 250 255 260 265 270 275 280 285 290 295 300 305 310 315 320 325 330 335 340 345 350 355 360 365 370 375 380 385 390 395 400 405 410 415 420 425 430 435 440 445 450 455 460 465 470 475 480 485 490 495 500 505 510 515 520 525 530 535 540 545 550 555 560 565 570 575 580 585 590 595 600 605 610 615 620 625 630 635 640 645 650 655 660 665 670 675 680 685 690 695 700 705 710 715 720 725 730 735 740 745 750 755 760 765 770 775 780 785 790 795 800 805 810 815 820 825 830 835 840 845 850 855 860 865 870 875 880 885 890 895 900 905 910 915 920 925 930 935 940 945 950 955 960 965 970 975 980 985 990 995 1000 1005 1010 1015 1020 1025 1030 1035 1040 1045 1050 1055 1060 1065 1070 1075 1080 1085 1090 1095 1100 1105 1110 1115 1120 1125 1130 1135 1140 1145 1150 1155 1160 1165 1170 1175 1180 1185 1190 1195 1200 1205 1210 1215 1220 1225 1230 1235 1240 1245 1250 1255 1260 1265 1270 1275 1280 1285 1290 1295 1300 1305 1310 1315 1320 1325 1330 1335 1340 1345 1350 1355 1360 1365 1370 1375 1380 1385 1390 1395 1400 1405 1410 1415 1420 1425 1430 1435 1440 1445 1450 1455 1460 1465 1470 1475 1480 1485 1490 1495 1500 1505 1510 1515 1520 1525 1530 1535 1540 1545 1550 1555 1560 1565 1570 1575 1580 1585 1590 1595 1600 1605 1610 1615 1620 1625 1630 1635 1640 1645 1650 1655 1660 1665 1670 1675 1680 1685 1690 1695 1700 1705 1710 1715 1720 1725 1730 1735 1740 1745 1750 1755 1760 1765 1770 1775 1780 1785 1790 1795 1800 1805 1810 1815 1820 1825 1830 1835 1840 1845 1850 1855 1860 1865 1870 1875 1880 1885 1890 1895 1900 1905 1910 1915 1920 1925 1930 1935 1940 1945 1950 1955 1960 1965 1970 1975 1980 1985 1990 1995 2000 2005 2010 2015 2020 2025 2030 2035 2040 2045 2050 2055 2060 2065 2070 2075 2080 2085 2090 2095 2100 2105 2110 2115 2120 2125 2130 2135 2140 2145 2150 2155 2160 2165 2170 2175 2180 2185 2190 2195 2200 2205 2210 2215 2220 2225 2230 2235 2240 2245 2250 2255 2260 2265 2270 2275 2280 2285 2290 2295 2300 2305 2310 2315 2320 2325 2330 2335 2340 2345 2350 2355 2360 2365 2370 2375 2380 2385 2390 2395 2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2485 2490 2495 2500 2505 2510 2515 2520 2525 2530 2535 2540 2545 2550 2555 2560 2565 2570 2575 2580 2585 2590 2595 2600 2605 2610 2615 2620 2625 2630 2635 2640 2645 2650 2655 2660 2665 2670 2675 2680 2685 2690 2695 2700 2705 2710 2715 2720 2725 2730 2735 2740 2745 2750 2755 2760 2765 2770 2775 2780 2785 2790 2795 2800 2805 2810 2815 2820 2825 2830 2835 2840 2845 2850 2855 2860 2865 2870 2875 2880 2885 2890 2895 2900 2905 2910 2915 2920 2925 2930 2935 2940 2945 2950 2955 2960 2965 2970 2975 2980 2985 2990 2995 3000 3005 3010 3015 3020 3025 3030 3035 3040 3045 3050 3055 3060 3065 3070 3075 3080 3085 3090 3095 3100 3105 3110 3115 3120 3125 3130 3135 3140 3145 3150 3155 3160 3165 3170 3175 3180 3185 3190 3195 3200 3205 3210 3215 3220 3225 3230 3235 3240 3245 3250 3255 3260 3265 3270 3275 3280 3285 3290 3295 3300 3305 3310 3315 3320 3325 3330 3335 3340 3345 3350 3355 3360 3365 3370 3375 3380 3385 3390 3395 3400 3405 3410 3415 3420 3425 3430 3435 3440 3445 3450 3455 3460 3465 3470 3475 3480 3485 3490 3495 3500 3505 3510 3515 3520 3525 3530 3535 3540 3545 3550 3555 3560 3565 3570 3575 3580 3585 3590 3595 3600 3605 3610 3615 3620 3625 3630 3635 3640 3645 3650 3655 3660 3665 3670 3675 3680 3685 3690 3695 3700 3705 3710 3715 3720 3725 3730 3735 3740 3745 3750 3755 3760 3765 3770 3775 3780 3785 3790 3795 3800 3805 3810 3815 3820 3825 3830 3835 3840 3845 3850 3855 3860 3865 3870 3875 3880 3885 3890 3895 3900 3905 3910 3915 3920 3925 3930 3935 3940 3945 3950 3955 3960 3965 3970 3975 3980 3985 3990 3995 4000 4005 4010 4015 4020 4025 4030 4035 4040 4045 4050 4055 4060 4065 4070 4075 4080 4085 4090 4095 4100 4105 4110 4115 4120 4125 4130 4135 4140 4145 4150 4155 4160 4165 4170 4175 4180 4185 4190 4195 4200 4205 4210 4215 4220 4225 4230 4235 4240 4245 4250 4255 4260 4265 4270 4275 4280 4285 4290 4295 4300 4305 4310 4315 4320 4325 4330 4335 4340 4345 4350 4355 4360 4365 4370 4375 4380 4385 4390 4395 4400 4405 4410 4415 4420 4425 4430 4435 4440 4445 4450 4455 4460 4465 4470 4475 4480 4485 4490 4495 4500 4505 4510 4515 4520 4525 4530 4535 4540 4545 4550 4555 4560 4565 4570 4575 4580 4585 4590 4595 4600 4605 4610 4615 4620 4625 4630 4635 4640 4645 4650 4655 4660 4665 4670 4675 4680 4685 4690 4695 4700 4705 4710 4715 4720 4725 4730 4735 4740 4745 4750 4755 4760 4765 4770 4775 4780 4785 4790 4795 4800 4805 4810 4815 4820 4825 4830 4835 4840 4845 4850 4855 4860 4865 4870 4875 4880 4885 4890 4895 4900 4905 4910 4915 4920 4925 4930 4935 4940 4945 4950 4955 4960 4965 4970 4975 4980 4985 4990 4995 5000 5005 5010 5015 5020 5025 5030 5035 5040 5045 5050 5055 5060 5065 5070 5075 5080 5085 5090 5095 5100 5105 5110 5115 5120 5125 5130 5135 5140 5145 5150 5155 5160 5165 5170 5175 5180 5185 5190 5195 5200 5205 5210 5215 5220 5225 5230 5235 5240 5245 5250 5255 5260 5265 5270 5275 5280 5285 5290 5295 5300 5305 5310 5315 5320 5325 5330 5335 5340 5345 5350 5355 5360 5365 5370 5375 5380 5385 5390 5395 5400 5405 5410 5415 5420 5425 5430 5435 5440 5445 5450 5455 5460 5465 5470 5475 5480 5485 5490 5495 5500 5505 5510 5515 5520 5525 5530 5535 5540 5545 5550 5555 5560 5565 5570 5575 5580 5585 5590 5595 5600 5605 5610 5615 5620 5625 5630 5635 5640 5645 5650 5655 5660 5665 5670 5675 5680 5685 5690 5695 5700 5705 5710 5715 5720 5725 5730 5735 5740 5745 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840 5845 5850 5855 5860 5865 5870 5875 5880 5885 5890 5895 5900 5905 5910 5915 5920 5925 5930 5935 5940 5945 5950 5955 5960 5965 5970 5975 5980 5985 5990 5995 6000 6005 6010 6015 6020 6025 6030 6035 6040 6045 6050 6055 6060 6065 6070 6075 6080 6085 6090 6095 6100 6105 6110 6115 6120 6125 6130 6135 6140 6145 6150 6155 6160 6165 6170 6175 6180 6185 6190 6195 6200 6205 6210 6215 6220 6225 6230 6235 6240 6245 6250 6255 6260 6265 6270 6275 6280 6285 6290 6295 6300 6305 6310 6315 6320 6325 6330 6335 6340 6345 6350 6355 6360 6365 6370 6375 6380 6385 6390 6395 6400 6405 6410 6415 6420 6425 6430 6435 6440 6445 6450 6455 6460 6465 6470 6475 6480 6485 6490 6495 6500 6505 6510 6515 6520 6525 6530 6535 6540 6545 6550 6555 6560 6565 6570 6575 6580 6585 6590 6595 6600 6605 6610 6615 6620 6625 6630 6635 6640 6645 6650 6655 6660 6665 6670 6675 6680 6685 6690 6695 6700 6705 6710 6715 6720 6725 6730 6735 6740 6745 6750 6755 6760 6765 6770 6775 6780 6785 6790 6795 6800 6805 6810 6815 6820 6825 6830 6835 6840 6845 6850 6855 6860 6865 6870 6875 6880 6885 6890 6895 6900 6905 6910 6915 6920 6925 6930 6935 6940 6945 6950 6955 6960 6965 6970 6975 6980 6985 6990 6995 7000 7005 7010 7015 7020 7025 7030 7035 7040 7045 7050 7055 7060 7065 7070 7075 7080 7085 7090 7095 7100 7105 7110 7115 7120 7125 7130 7135 7140 7145 7150 7155 7160 7165 7170 7175 7180 7185 7190 7195 7200 7205 7210 7215 7220 7225 7230 7235 7240 7245 7250 7255 7260 7265 7270 7275 7280 7285 7290 7295 7300 7305 7310 7315 7320 7325 7330 7335 7340 7345 7350 7355 7360 7365 7370 7375 7380 7385 7390 7395 7400 7405 7410 7415 7420 7425 7430 7435 7440 7445 7450 7455 7460 7465 7470 7475 7480 7485 7490 7495 7500 7505 7510 7515 7520 7525 7530 7535 7540 7545 7550 7555 7560 7565 7570 7575 7580 7585 7590 7595 7600 7605 7610 7615 7620 7625 7630 7635 7640 7645 7650 7655 7660 7665 7670 7675 7680 7685 7690 7695 7700 7705 7710 7715 7720 7725 7730 7735 7740 7745 7750 7755 7760 7765 7770 7775 7780 7785 7790 7795 7800 7805 7810 7815 7820 7825 7830 7835 7840 7845 7850 7855 7860 7865 7870 7875 7880 7885 7890 7895 7900 7905 7910 7915 7920 7925 7930 7935 7940 7945 7950 7955 7960 7965 7970 7975 7980 7985 7990 7995 8000 8005 8010 8015 8020 8025 8030 8035 8040 8045 8050 8055 8060 8065 8070 8075 8080 8085 8090 8095 8100 8105 8110 8115 8120 8125 8130 8135 8140 8145 8150 8155 8160 8165 8170 8175 8180 8185 8190 8195 8200 8205 8210 8215 8220 8225 8230 8235 8240 8245 8250 8255 8260 8265 8270 8275 8280 8285 8290 8295 8300 8305 8310 8315 8320 8325 8330 8335 8340 8345 8350 8355 8360 8365 8370 8375 8380 8385 8390 8395 8400 8405 8410 8415 8420 8425 8430 8435 8440 8445 8450 8455 8460 8465 8470 8475 8480 8485 8490 8495 8500 8505 8510 8515 8520 8525 8530 8535 8540 8545 8550 8555 8560 8565 8570 8575 8580 8585 8590 8595 8600 8605 8610 8615 8620 8625 8630 8635 8640 8645 8650 8655 8660 8665 8670 8675 8680 8685 8690 8695 8700 8705 8710 8715 8720 8725 8730 8735 8740 8745 8750 8755 8760 8765 8770 8775 8780 8785 8790 8795 8800 8805 8810 8815 8820 8825 8830 8835 8840 8845 8850 8855 8860 8865 8870 8875 8880 8885 8890 8895 8900 8905 8910 8915 8920 8925 8930 8935 8940 8945 8950 8955 8960 8965 8970 8975 8980 8985 8990 8995 9000 9005 9010 9015 9020 9025 9030 9035 9040 9045 9050 9055 9060 9065 9070 9075 9080 9085 9090 9095 9100 9105 9110 9115 9120 9125 9130 9135 9140 9145 9150 9155 9160 9165 9170 9175 9180 9185 9190 9195 9200 9205 9210 9215 9220 9225 9230 9235 9240 9245 9250 9255 9260 9265 9270 9275 9280 9285 9290 9295 9300 9305 9310 9315 9320 9325 9330 9335 9340 9345 9350 9355 9360 9365 9370 9375 9380 9385 9390 9395 9400 9405 9410 9415 9420 9425 9430 9435 9440 9445 9450 9455 9460 9465 9470 9475 9480 9485 9490 9495 9500 9505 9510 9515 9520 9525 9530 9535 9540 9545 9550 9555 9560 9565 9570 9575 9580 9585 9590 9595 9600 9605 9610 9615 9620 9625 9630 9635 9640 9645 9650 9655 9660 9665 9670 9675 9680 9685 9690 9695 9700 9705 9710 9715 9720 9725 9730 9735 9740 9745 9750 9755 9760 9765 9770 9775 9780 9785 9790 9795 9800 9805 9810 9815 9820 9825 9830 9835 9840 9845 9850 9855 9860 9865 9870 9875 9880 9885 9890 9895 9900 9905 9910 9915 9920 9925 9930 9935 9940 9945 9950 9955 9960 9965 9970 9975 9980 9985 9990 9995 10000 10005 10010 10015 10020 10025 10030 10035 10040 10045 10050 10055 10060 10065 10070 10075 10080 10085 10090 10095 10100 10105 10110 10115 10120 10125 10130 10135 10140 10145 10150 10155 10160 10165 10170 10175 10180 10185 10190 10195 10200 10205 10210 10215 10220 10225 10230 10235 10240 10245 10250 10255 10260 10265 10270 10275 10280 10285 10290 10295 10300 10305 10310 10315 10320 10325 10330 10335 10340 10345 10350 10355 10360 10365 10370

off. The central processing unit MCU sets the control line of the display unit control means 9 to a logical "1" value (for example ca. 3 V) when the cipher mode is on. Acoustic signal formation can be applied in a corresponding manner. Thus the central processing unit MCU sets the control line of the control means 11 for the acoustic signal forming element (not shown) to a logical "0" value, when there are no changes in the cipher mode. When the cipher mode is changed, the central processing unit MCU sets said control line for a moment to a logical "1" value and resets said control line to an "0" value after a suitable length of time. Thus the length of the acoustic signal can be influenced by the duration of the "1" value state.

Data transmission between different blocks in the apparatus according to the invention can be arranged using methods known as such, wherein it is unnecessary to explain it in more detail in this context.

The method of the present invention can be advantageously applied also in mobile stations currently in use in a way that the functions required in the method are provided in the operational software of the mobile station. Thus no changes will be required in the hardware of the mobile station.

The invention can also be applied in a way that part of the functions required in the method are provided in the operational software of the mobile station and part of them are provided in the software of a data processor which is in transmission connection with the mobile station. One such embodiment is illustrated as a reduced block diagram in Fig. 6.

In this embodiment, the mobile station is also used as a so-called wireless modem in connection with a data processor, such as a personal computer, wherein a data transmission connection is formed from the data processor PC via the mobile communication network e.g. to another data processor. In this case, it is advantageous to indicate the cipher mode as a certain sign on the display 12 of the data processor and possibly also as an acoustic signal by the acoustic signal forming element 13 of the data processor. The cipher indicator memory block 2 transmits information on a change in the cipher indication data field advantageously to the data processor PC by means of a mobile station connection element 14 and a PC connection bus 15. The data processor PC is provided with application software which controls that the data on the change in the cipher indication data field is read in the data processor PC from a data processor connection element 16 and processed preferably in the central processing unit 17 of the data processor. After this the data processor PC sends out a cipher mode enquiry message which is transmitted back to the cipher indicator memory block by means of the data processor connection element 16, the PC connection bus 15 and the mobile station connection element 14. In response to the enquiry message, the cipher indicator memory block 2 sends the cipher data to the data processor PC. From the data processor PC, the cipher data is read

from the data processor connection element 16 and transmitted to the cipher mode indicator. The cipher mode indicator is preferably the display unit 12 and possibly also the acoustic signal forming element 13 of the data processor. Thus the cipher mode is indicated by a suitable symbol on the display unit 12 of the data processor. In a corresponding way, a change in the cipher mode is indicated e.g. as an acoustic signal by the acoustic signal forming element 13 of the data processor. Also the operation and structure of the data processor PC are generally known and need not be explained in more detail in this context.

Further, the invention can be applied in situations where a data transmission connection (call) is formed between two mobile stations. Thus data transmission between the first mobile station MS1 and a mobile communication network as well as between the second mobile station MS2 and a mobile communication network takes place via the radio channel. The mobile stations MS1, MS2 can be located in areas of different base stations, wherein it is possible that the cipher mode in communication between the first mobile station MS1 and the mobile network is different than in communication between the second mobile station MS2 and the mobile network. The data transmission connection between the first mobile station MS1 and the second mobile station MS2 is formed in a way known as such. After the connection has been made, it is possible e.g. for the first mobile station MS1 to enquire the cipher mode of the second mobile station MS2 (Fig. 8). The enquiry can be made for example as call control signalling, such as in the GSM mobile network, and also if the ISDN between the mobile services switching centres MSC is in the user-user information element according to the GSM Standard 04.08. The resources control block 1 of the first mobile station MS1 forms a cipher mode enquiry message and transmits it to the second mobile station. The resource control block 18 of the second mobile station detects the cipher mode of the second mobile station and forms a response message where the cipher mode is transmitted to the resource control block 1 of the first mobile station. After this, the resource control block 1 of the first mobile station MS1 sets the cipher indication data field as disclosed above in this description. The first mobile station MS1 can also be provided with a second cipher indication data field for recording cipher data between the second mobile station MS2 and the mobile communication network. Thus the user of the mobile station MS1, MS2 can be given the cipher mode separately for communication between the first mobile station MS1 and the mobile network and for communication between the second mobile station MS2 and the mobile network. In another alternative, the user of the mobile station MS1, MS2 is given the cipher mode so that if communication between both mobile stations MS1, MS2 and the mobile network is enciphered, the user of the mobile station MS1, MS2 is informed that the cipher mode is on. In a different case the user is in-

formed that the cipher mode is off.

If the cipher mode in the second mobile station MS2 is changed during a call, it sends a message on the change in the cipher mode by user-user signalling.

For enquiring the cipher mode of communication [to and from] the second mobile station MS2, also other methods can be used, such as short message services (SMS).

The ISDN telecommunication network (Integrated Services Digital Network) provides also an optional user-to-user signalling service (UUS) which makes communication possible between telecommunication terminals in a data transmission connection with each other. Thus, if a data transmission connection is made from a mobile station MS to a telecommunication terminal of the ISDN type, the mobile station MS can send the telecommunication terminal an enquiry about the cipher mode by using the user-to-user signalling service. If the telecommunication terminal does not recognize the enquiry message of the mobile station MS, the mobile station MS will not receive a response to the enquiry, or the response will consist of an unidentified command or another corresponding message. In such a case, the mobile station MS can deduce that the telecommunication terminal is not a mobile station but most probably a telecommunication terminal connected with a landline telecommunication network. In this situation, the display unit of the mobile station MS indicates the user of the mobile station for example that the cipher mode between the second telecommunication terminal and the telecommunication network is unknown.

For indicating the cipher mode and a change in the cipher mode to the user of the mobile station MS, also other methods, known as such, can be used. For example, the cipher mode can be indicated by a light source, such as a light-emitting diode (LED). Consequently, for example when the cipher mode is on, a control voltage is supplied to the LED (the LED is emitting) and when the communication is not enciphered, no control voltage is supplied to the LED (the LED is unlit). A change in the cipher mode can be advantageously indicated by flashing the LED. Thus for example when the communication is not enciphered, the LED is unlit, and when the communication becomes enciphered, the LED flashes for a moment after which the LED will emit light continuously as long as the cipher mode is on. In a corresponding manner, when the communication becomes unenciphered, the LED will flash for a moment before it is turned off.

Further, so-called vibration batteries have been developed for mobile stations whereby the mobile station can be made to vibrate in a muffled way. Thus the cipher mode of data transmission can be indicated also by a vibration battery, wherein for example upon a change in the cipher mode, a control signal is supplied to the vibration battery for a moment, which will result in vibration of the mobile station and detection of the change in the cipher mode by the user of the mobile station.

The invention is not limited only to the embodiments presented above, but it can be modified within the scope of the appended claims.

5

Claims

1. A method for indicating enciphering of data transmission between a mobile communication network and a mobile station (MS) in the mobile communication network, characterized in that
 - signals transferred between a mobile communication network and a mobile station are monitored, and
 - on the basis of the signal monitored, the cipher mode is indicated to the user of the mobile station.
2. A method according to claim 1, characterized in that in addition to indicating the cipher mode, a change in the cipher mode is indicated to the user of the mobile station.
3. A method according to claim 1 or 2, characterized in that the data transmission connection between the mobile communication network and the mobile station (MS) is a radio connection.
4. A method according to any of the claims 1 to 3, characterized in that the communication network is a digital communication network, such as a GSM network.
5. A method according to any of the claims 1 to 4, wherein the mobile station (MS) comprises a display unit (8) and an acoustic signal forming element (10), known as such, characterized in that the cipher mode is indicated with the display unit (8) and a change in the cipher mode is indicated with the acoustic signal forming element (10).
6. A method according to any of the claims 1 to 4, wherein the mobile station (MS) comprises a light source (LED), known as such, characterized in that the cipher mode is indicated with the light source (LED).
7. A method according to claim 6, characterized in that a change in the cipher mode is indicated with a flashing light.
8. A method according to any of the claims 1 to 4, characterized in that the cipher mode is indicated by vibration.
9. A method according to any of the preceding claims,

- characterized** in that the signal to be monitored is a control signal.
10. A method according to any of the preceding claims, wherein a first mobile station (MS1) and a second mobile station (MS2) are in a data transmission connection with each other through at least one mobile communication network, **characterized** in that the cipher mode between the mobile communication network and the first mobile station (MS1) is indicated to the user of the second mobile station (MS2). 10
11. A method according to any of the preceding claims, wherein the mobile station is used in connection with a data processor (PC) for data transmission between a mobile communication network and the data processor (PC), **characterized** in that the cipher mode is indicated on the display unit (12) of the data processor and a change in the cipher mode is indicated with the acoustic signal forming element (10) of the data processor. 15
12. An apparatus for indicating enciphering of data transmission between a mobile station (MS) and a mobile communication network in the mobile communication network, **characterized** in that the apparatus comprises: 25
- means (1) for monitoring signals transferred between a mobile communication network and a mobile station (MS) and
 - means (8, 12) for indicating the cipher mode to the user of the mobile station.
- 30
13. An apparatus according to claim 12, **characterized** in that the apparatus comprises further means (10, 13) for indicating a change in the cipher mode. 35
14. An apparatus according to claim 12 or 13, **characterized** in that the means (8, 12) for indicating the cipher mode comprise a display unit (8) of the mobile station, and the means (10, 13) for indicating a change in the cipher mode comprise an acoustic signal forming element (10), such as a sound generator or the like. 40
15. An apparatus according to any of the claims 12 to 14, **characterized** in that the means (10, 13) for indicating a change in the cipher mode comprise a light source (LED), known as such. 45
16. An apparatus according to any of the claims 12 to 15, **characterized** in that the means (10, 13) for indicating a change in the cipher mode comprise means for generating vibration. 50
17. An apparatus according to any of the claims 12 to 55
- 16, **characterized** in that it is provided in a mobile station (MS).
- 5
18. An apparatus according to claim 12 or 13, **characterized** in that the means (8, 12) for indicating the cipher mode and the means (10, 13) for indicating a change in the cipher mode are provided in a data processor (PC) communicating with a mobile station (MS).
- 10

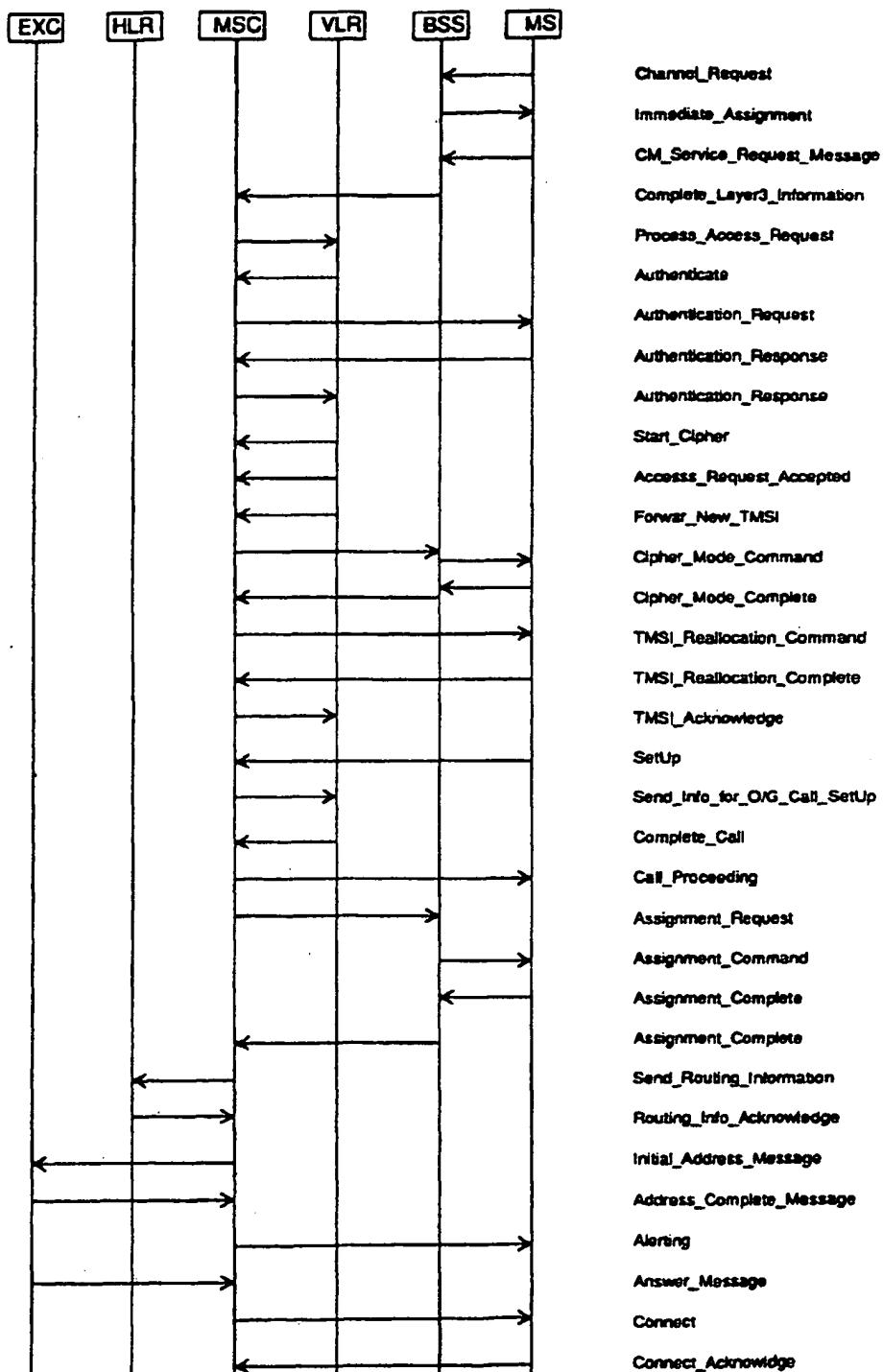


Fig. 1a

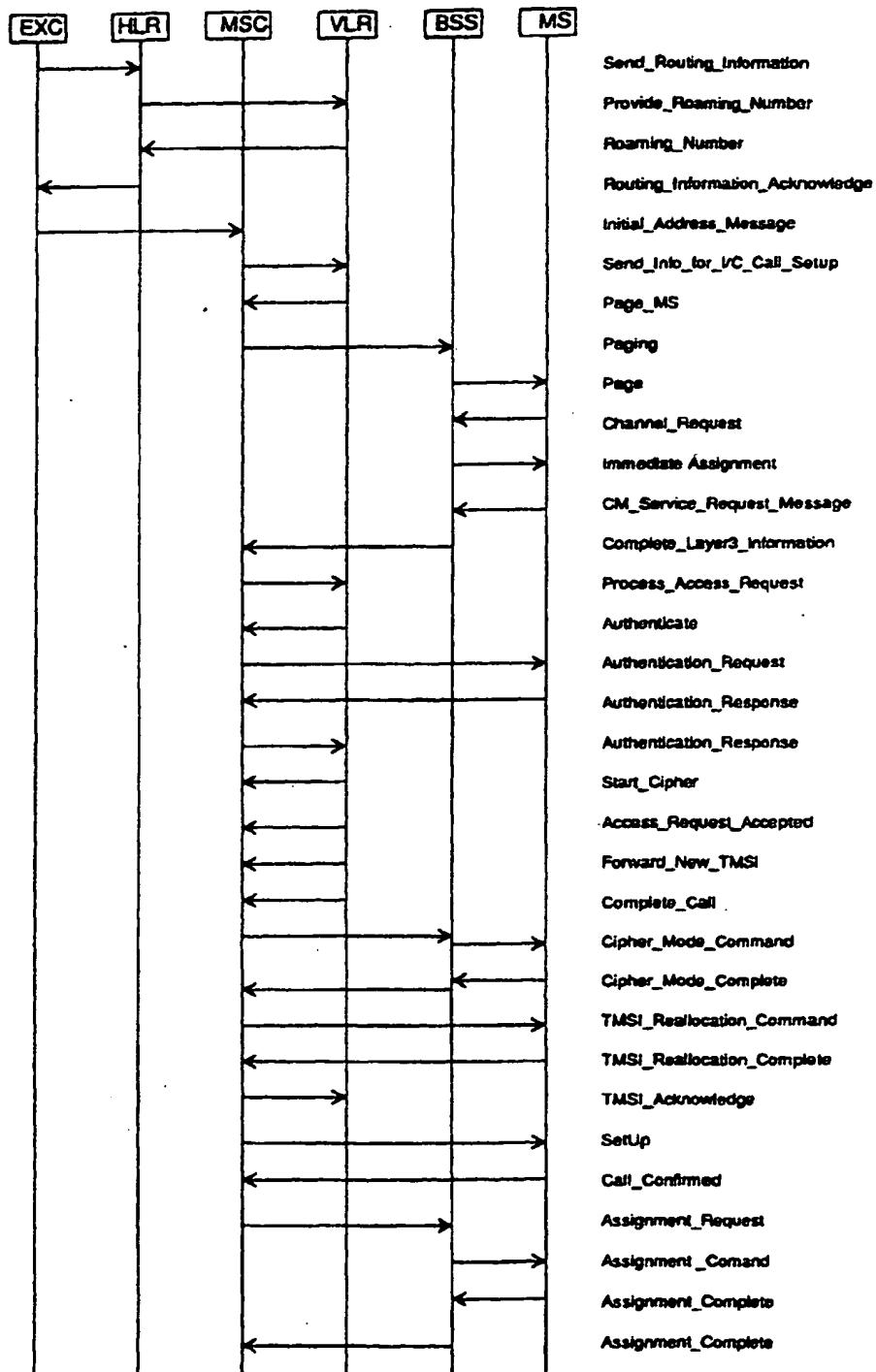


Fig. 1b

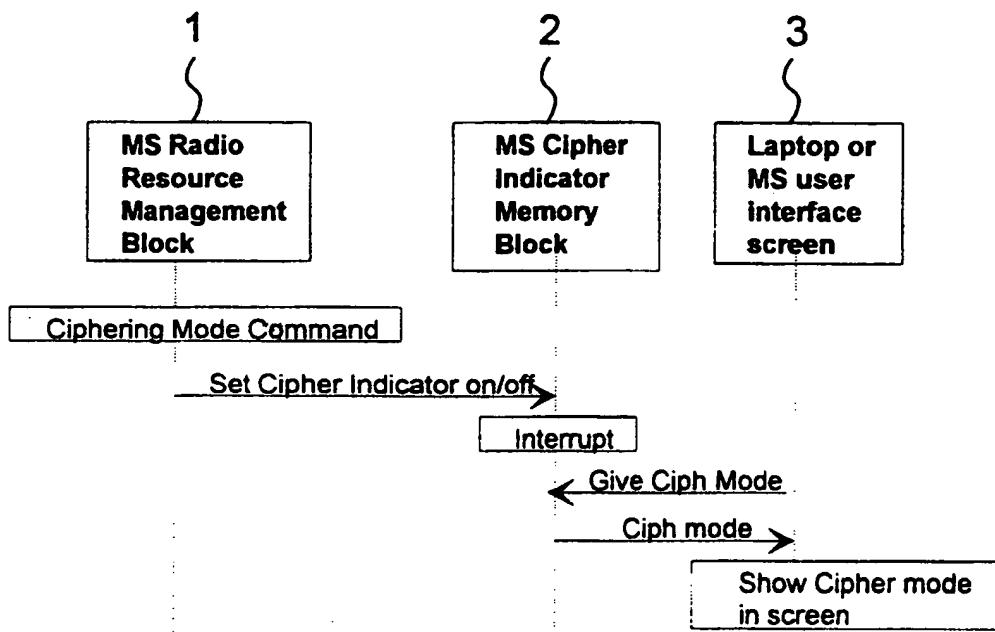


Fig. 2

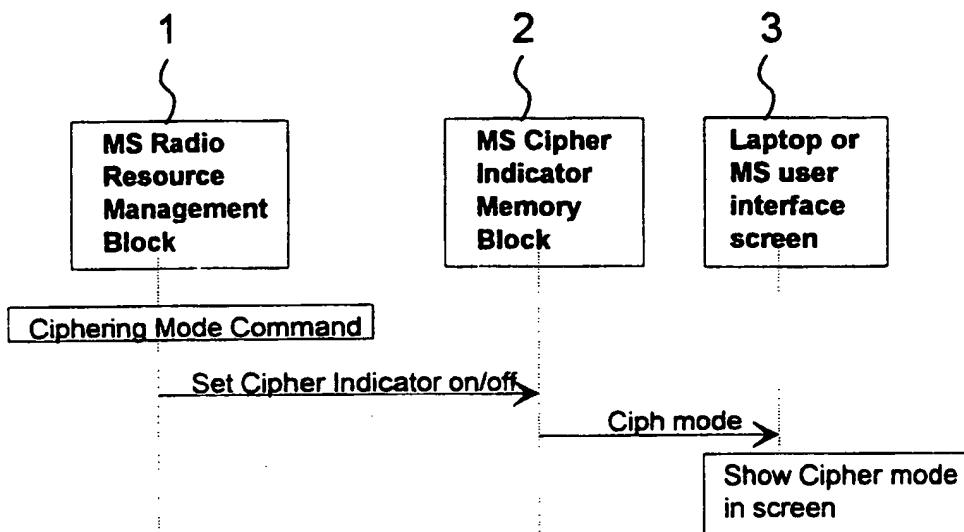


Fig. 3

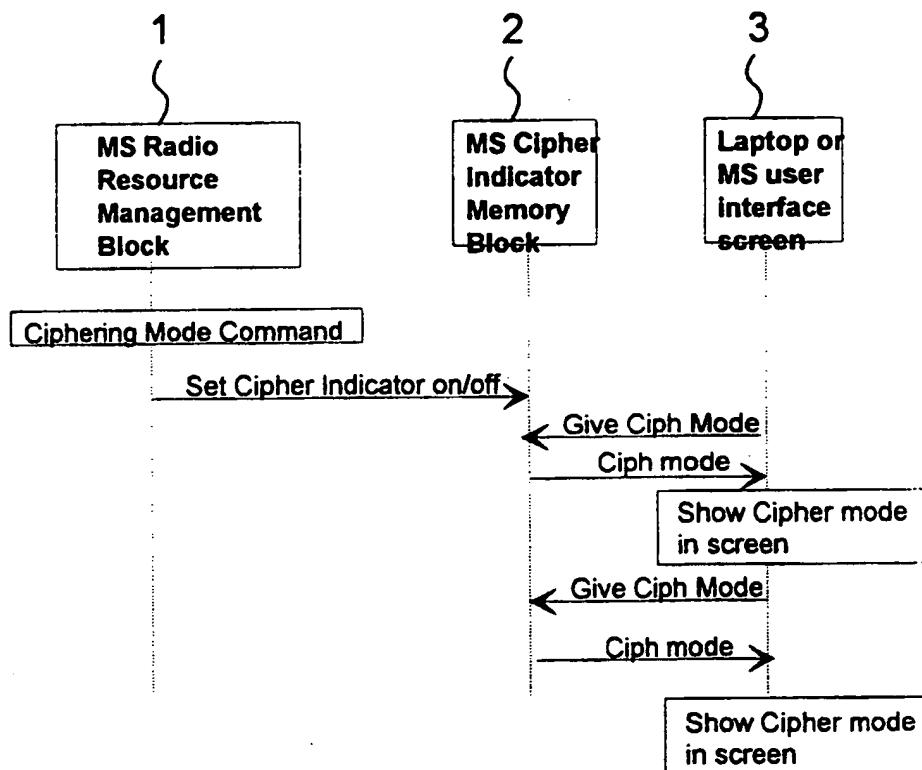


Fig. 4

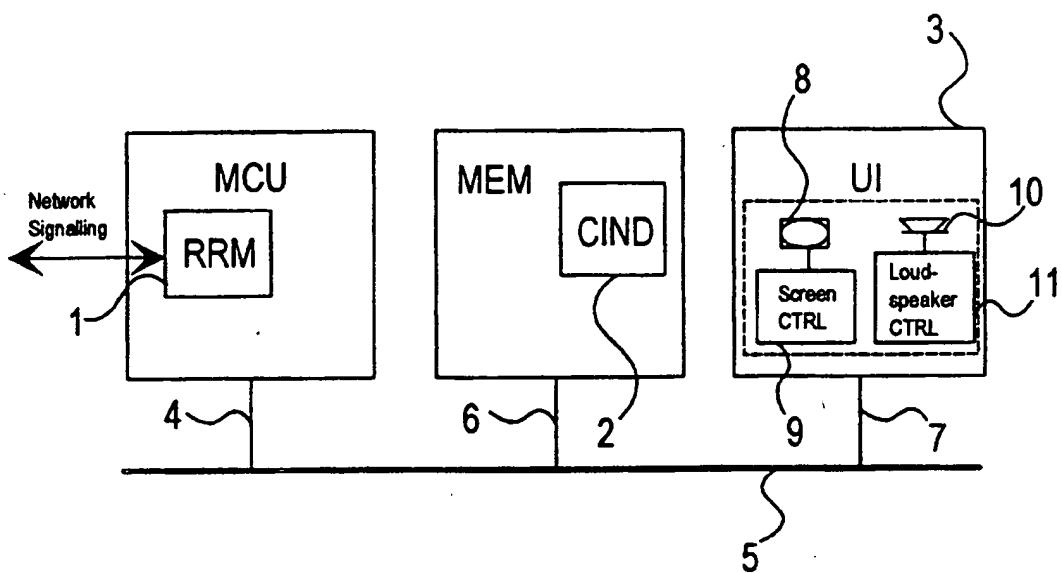


Fig. 5

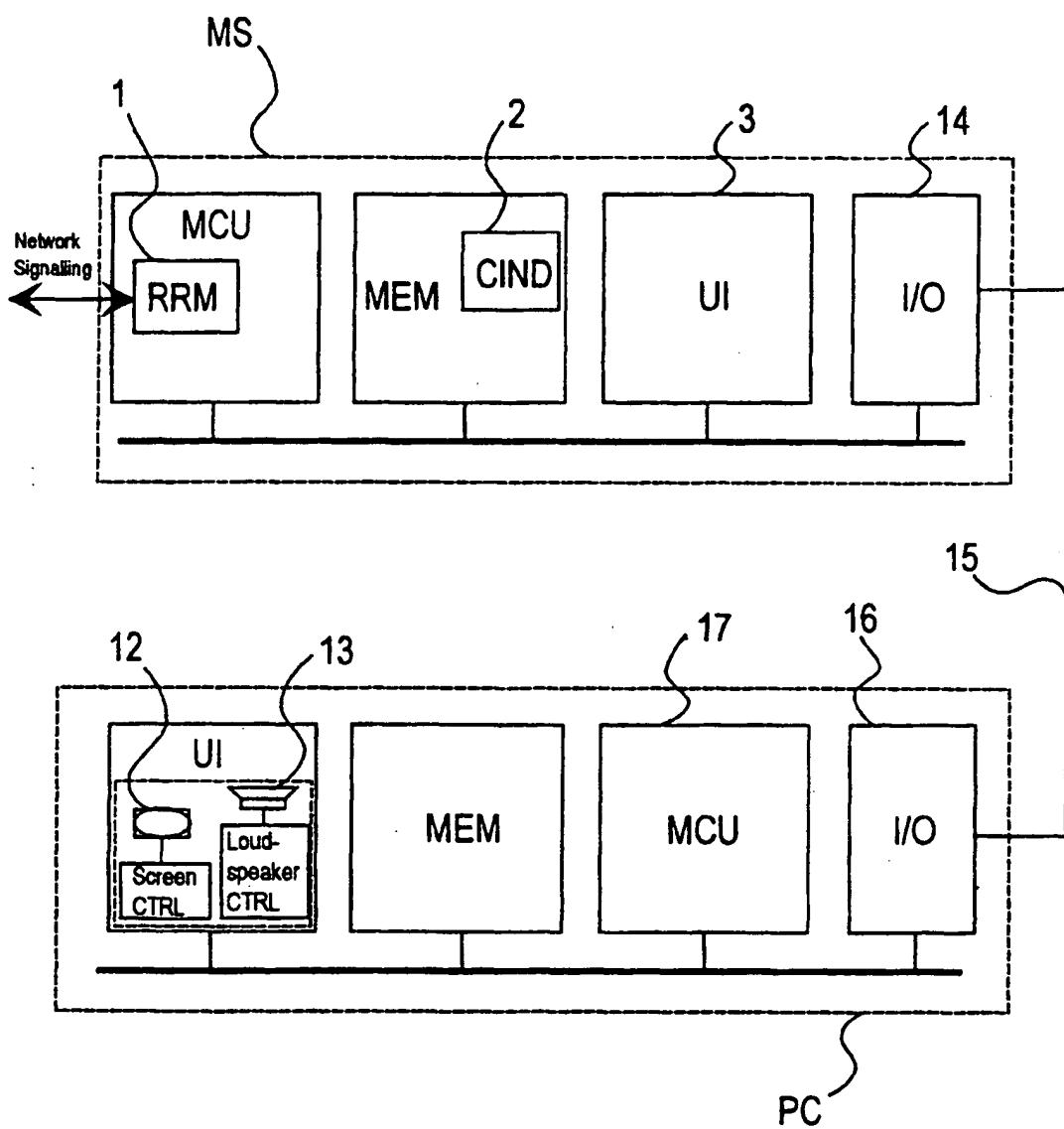


Fig. 6

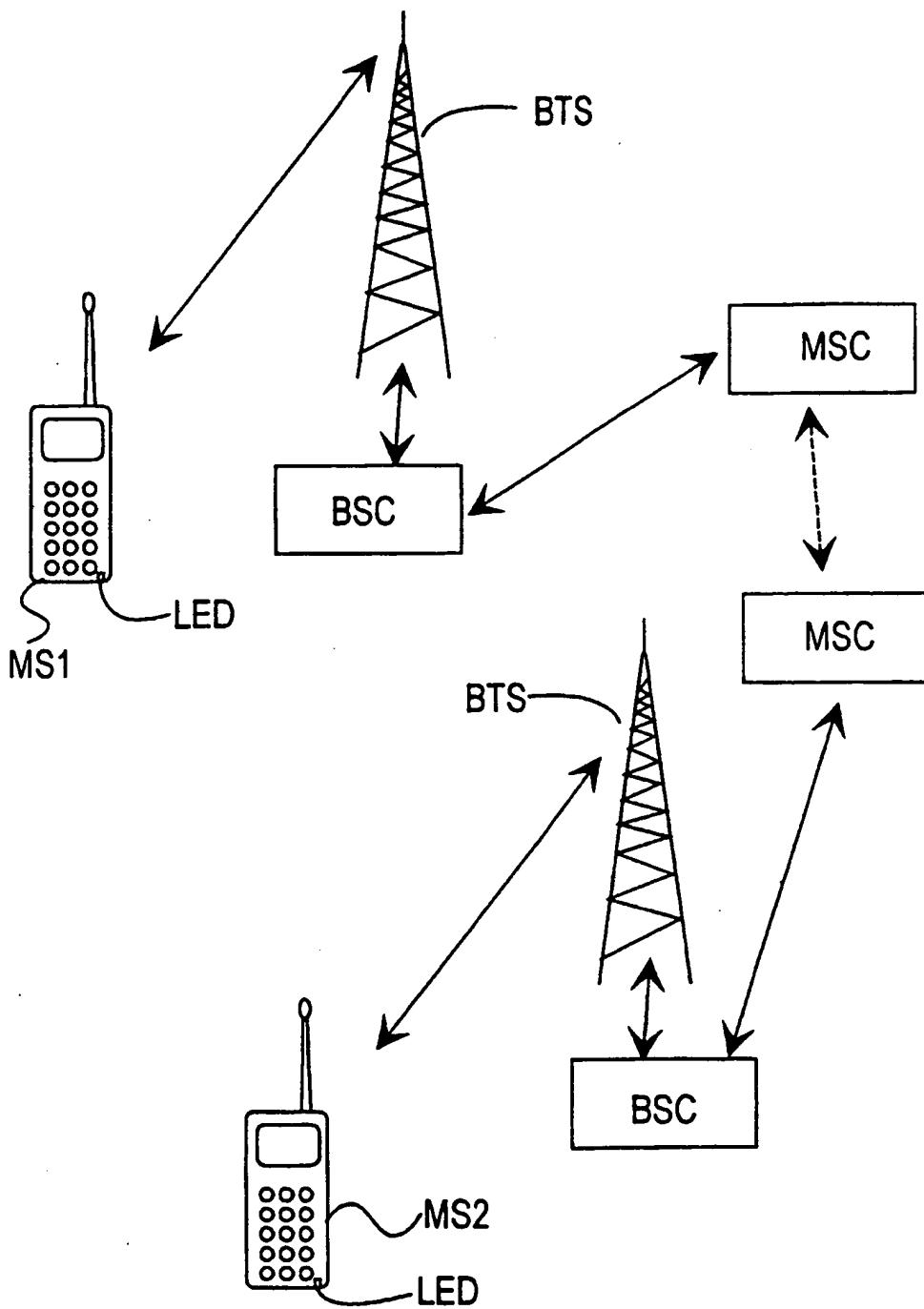


Fig. 7

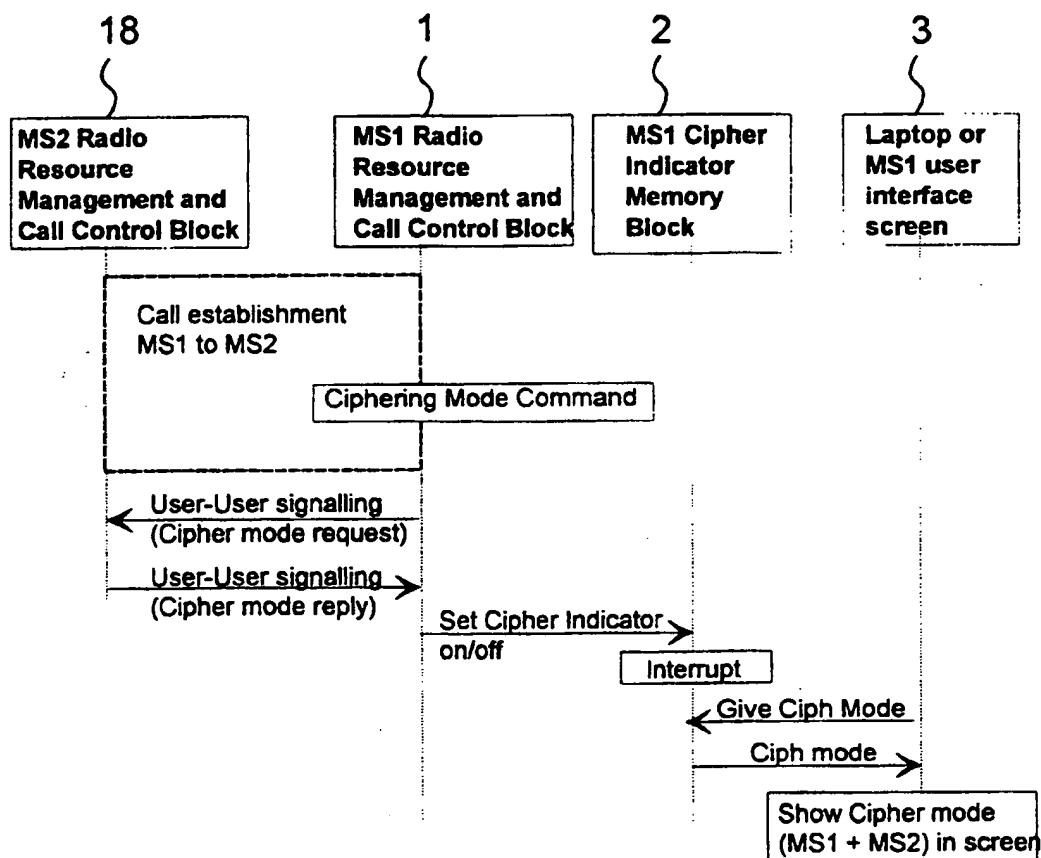


Fig. 8